(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 619 856 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
02.07.2008 Bulletin 2008/27

(51) Int Cl.:
H04L 29/06 *(2006.01)* ***G06F 1/00*** *(2006.01)*

(21) Application number: **05020603.6**

(22) Date of filing: **14.05.2002**

(54) Method and system for controlling the scope of delegation of authentication credentials

Verfahren und System zur Steuerung des Umfangs der Delegierung von Authentifizierungsdaten

Procédé et système de contrôle de l'étendue de la délégation des données d'authentification

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

(30) Priority: **20.06.2001 US 886146**

(43) Date of publication of application:
25.01.2006 Bulletin 2006/04

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
02010767.8 / 1 271 882

(73) Proprietor: **MICROSOFT CORPORATION**
Redmond, Washington 98052-6399 (US)

(72) Inventors:
- **Brezak, John E.**
  Woodinville
  WA 98072 (US)
- **Ward, Richard B.**
  Redmond
  WA 98053 (US)
- **Schmidt, Donald E.**
  Redmond
  WA 98052 (US)

(74) Representative: **Grünecker, Kinkeldey,**
Stockmair & Schwanhäusser
Anwaltssozietät
Leopoldstrasse 4
80802 München (DE)

(56) References cited:
US-A- 5 590 199

- **MCMAHON P V: "SESAME V2 public key and authorisation extensions to Kerberos" NETWORK AND DISTRIBUTED SYSTEM SECURITY, 1995., PROCEEDINGS OF THE SYMPOSIUM ON SAN DIEGO, CA, USA 16-17 FEB. 1995, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, 16 February 1995 (1995-02-16), pages 114-131, XP010134534 ISBN: 0-8186-7027-4**
- **PIESSENS F ET AL: "Interconnecting domains with heterogeneous key distribution and authentication protocols" RESEARCH IN SECURITY AND PRIVACY, 1993. PROCEEDINGS., 1993 IEEE COMPUTER SOCIETY SYMPOSIUM ON OAKLAND, CA, USA 24-26 MAY 1993, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 24 May 1993 (1993-05-24), pages 66-79, XP010094851 ISBN: 0-8186-3370-0**
- **TROSTLE J T ET AL: "A flexible distributed authorization protocol" NETWORK AND DISTRIBUTED SYSTEM SECURITY, 1996., PROCEEDINGS OF THE SYMPOSIUM ON SAN DIEGO, CA, USA 22-23 FEB. 1996, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 22 February 1996 (1996-02-22), pages 43-52, XP010158984 ISBN: 0-8186-7222-6**

EP 1 619 856 B1

Description

TECHNICAL FIELD

[0001] This invention relates generally to computer access control, and more particularly to methods and systems for controlling the scope of delegation of authentication credentials.

BACKGROUND

[0002] Access control is paramount to computer security. To protect the integrity of computer systems and the confidentiality of important data, various access control schemes have been implemented to prevent unauthorized users and malicious attackers from gaining access to computer resources.

[0003] To ensure the comprehensiveness of computer security, access control is often implemented on various levels. For instance, on the level of one computer, a user is typically required to go through a logon procedure in which the computer determines whether the user is authorized to use the computer. In addition, on the level of a computer network, a user is commonly required to go through a user-authentication process for purposes of controlling the user's access to various network services. Even after a network access control server has authenticated the user, the user may still have to request a permit for a specific server in order to access that service. Various schemes based on different protocols, such as the Kerberos 5 protocol, have been proposed and implemented for controlling network access control by means of user authentication.

[0004] Generally, the user logon for a computer and the user authentication for network access control are two separate procedures. Nevertheless, to minimize the burden on a user in dealing with the different access control schemes, the user logon and the user authentication for network access are sometimes performed together. For example, in the case where the user authentication is implemented under the Kerberos protocol, when the user logs on the computer, the computer may also initiate a Kerberos authentication process. In the authentication process, the computer contacts a Kerberos Key Distribution Center (KDC) to first obtain a ticket-granting ticket (TGT) for the user. The computer can then use the TGT to obtain from the KDC, a session ticket for itself.

[0005] As networks have evolved, there has been a trend to have multiple tiers of server/service computers arranged to handle client computer requests. A simple example is a client computer making a request to a World Wide Web website via the Internet. Here, there may be a front-end web server that handles the formatting and associated business rules of the request, and a back-end server that manages a database for the website. For additional security, the web site may be configured such that an authentication protocol forwards (or delegates) credentials, such as, e.g., the user's TGT, and/or possibly other information from the front-end server to a back-end server. This practice is becoming increasingly common in many websites, and/or other multiple-tiered networks.

[0006] Thus, any server/computer in possession of the user's TGT and associated authenticator can request tickets on behalf of the user/client from the KDC. This capability is currently used to provide forwarded ticket delegation. Unfortunately, such delegation to a server is essentially unconstrained for the life of the TGT. Consequently, there is a need for improved methods and systems that support delegation of authentication credentials in complex network configurations, but in a more constrained manner.

[0007] Furthermore, it is known from "SESAME V2 Public Key and Authorization Extensions to Kerberos", by McMahon P.V., February 16, 1995, public key and authorization extensions to Kerberos. In particular, the integration of asymmetric key distribution and authorization support to extend Kerberos is described. Moreover, it is described as a primary extension the support of asymmetric inter-realm key distribution to make scalable secure interworking practical between the remote realms. In addition, a scheme is defined for securely propagating principle privileges, including roles and groups, from clients to servers in order to reduce access control management overheads at end-systems, but provide policy control safeguards to limit which applications can be accessed and which, if any, can act as delegates.

[0008] Further, it is known from "Interconnecting Domains with Heterogeneous Key Distribution and Authentication Protocols" by Piessens, F., De Decker, B., and Janson, P. mechanisms that can be used in the design of a protocol convertor for authentication and key distribution protocols. It is, described that a first mechanism, based on proxies and a synchronization protocol, allows for a transparent protocol conversion. Moreover, it is described that a second mechanism addresses the problem of the statefulness of the protocol convertor. It these mechanisms that, when properly combined, provide for a robust, transparent and safe protocol convertor for authentication and key distribution protocols.

[0009] Therefore, it is the object of the invention to provide improved methods and systems for providing constrained delegation of authentication credentials.

[0010] This object is solved by the subject matter of the independent claims.

[0011] Preferred embodiments are the subject of the dependent claims.

[0012] Improved methods and systems are provided herein, which provide constrained delegation of authentication credentials.

[0013] The above stated needs and others are met, for example, by a method that includes identifying a target service to which access is sought on behalf of a client, and causing a server to request a new service credential, for use by the server, from a trusted third-party. To accomplish this, the server provides the trusted third-party with a credential authenticating the server, information

about the target service, and a service credential previously obtained by the client, or by the server on behalf of the client. Here, the new service credential is granted in the identity of the client rather than that of the server, but can only be used by the server to gain access to the target service.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] A more complete understanding of the various methods and systems of the present invention may be had by reference to the following detailed description when taken in conjunction with the accompanying drawings wherein:

Fig. 1 is a block diagram generally illustrating an exemplary computer system on which the present invention may be implemented.

Fig. 2 is a block diagram depicting a service-for-user-to-proxy (S4U2proxy) process performed within a client-server environment, in accordance with certain exemplary implementations of the present invention.

Fig. 3A is a block diagram depicting a service-for-user-to-self (S4U2self) process performed within a client-server environment, in accordance with certain exemplary implementations of the present invention.

Fig. 3B is a block diagram depicting a service-for-user-to-self (S4U2self) process performed within a client-server environment, in accordance with certain further exemplary implementations of the present invention.

Fig. 4 is an illustrative diagram depicting selected portions of a message format suitable for use with certain implementations of the present invention.

DETAILED DESCRIPTION

[0015] Turning to the drawings, wherein like reference numerals refer to like elements, the invention is illustrated as being implemented in a suitable computing environment. Although not required, the invention will be described in the general context of computer-executable instructions, such as program modules, being executed by a personal computer. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Moreover, those skilled in the art will appreciate that the invention may be practiced with other computer system configurations, including hand-held devices, multi-processor systems, microprocessor based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and the like. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

[0016] Fig.1 illustrates an example of a suitable computing environment 120 on which the subsequently described methods and systems may be implemented.

[0017] Exemplary computing environment 120 is only one example of a suitable computing environment and is not intended to suggest any limitation as to the scope of use or functionality of the improved methods and systems described herein. Neither should computing environment 120 be interpreted as having any dependency or requirement relating to any one or combination of components illustrated in computing environment 120.

[0018] The improved methods and systems herein are operational with numerous other general purpose or special purpose computing system environments or configurations. Examples of well known computing systems, environments, and/or configurations that may be suitable include, but are not limited to, personal computers, server computers, thin clients, thick clients, hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, set top boxes, programmable consumer electronics, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like.

[0019] As shown in Fig. 1, computing environment 120 includes a general-purpose computing device in the form of a computer 130. The components of computer 130 may include one or more processors or processing units 132, a system memory 134, and a bus 136 that couples various system components including system memory 134 to processor 132.

[0020] Bus 136 represents one or more of any of several types of bus structures, including a memory bus or memory controller, a peripheral bus, an accelerated graphics port, and a processor or local bus using any of a variety of bus architectures. By way of example, and not limitation, such architectures include Industry Standard Architecture (ISA) bus, Micro Channel Architecture (MCA) bus, Enhanced ISA (EISA) bus, Video Electronics Standards Association (VESA) local bus, and Peripheral Component Interconnects (PCI) bus also known as Mezzanine bus.

[0021] Computer 130 typically includes a variety of computer readable media. Such media may be any available media that is accessible by computer 130, and it includes both volatile and non-volatile media, removable and non-removable media.

[0022] In Fig. 1, system memory 134 includes computer readable media in the form of volatile memory, such as random access memory (RAM) 140, and/or non-volatile memory, such as read only memory (ROM) 138. A basic input/output system (BIOS) 142, containing the basic routines that help to transfer information between elements within computer 130, such as during start-up, is stored in ROM 138. RAM 140 typically contains data and/or program modules that are immediately accessible to and/or presently being operated on by processor 132.

[0023] Computer 130 may further include other remov-

able/non-removable, volatile/non-volatile computer storage media. For example, Fig. 1 illustrates a hard disk drive 144 for reading from and writing to a non-removable, non-volatile magnetic media (not shown and typically called a "hard drive"), a magnetic disk drive 146 for reading from and writing to a removable, non-volatile magnetic disk 148 (e.g., a "floppy disk"), and an optical disk drive 150 for reading from or writing to a removable, non-volatile optical disk 152 such as a CD-ROM, CD-R, CD-RW, DVD-ROM, DVD-RAM or other optical media. Hard disk drive 144, magnetic disk drive 146 and optical disk drive 150 are each connected to bus 136 by one or more interfaces 154.

[0024] The drives and associated computer-readable media provide nonvolatile storage of computer readable instructions, data structures, program modules, and other data for computer 130. Although the exemplary environment described herein employs a hard disk, a removable magnetic disk 148 and a removable optical disk 152, it should be appreciated by those skilled in the art that other types of computer readable media which can store data that is accessible by a computer, such as magnetic cassettes, flash memory cards, digital video disks, random access memories (RAMs), read only memories (ROM), and the like, may also be used in the exemplary operating environment.

[0025] A number of program modules may be stored on the hard disk, magnetic disk 148, optical disk 152, ROM 138, or RAM 140, including, e.g., an operating system 158, one or more application programs 160, other program modules 162, and program data 164.

[0026] The improved methods and systems described herein may be implemented within operating system 158, one or more application programs 160, other program modules 162, and/or program data 164.

[0027] A user may provide commands and information into computer 130 through input devices such as keyboard 166 and pointing device 168 (such as a "mouse"). Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, serial port, scanner, camera, etc. These and other input devices are connected to the processing unit 132 through a user input interface 170 that is coupled to bus 136, but may be connected by other interface and bus structures, such as a parallel port, game port, or a universal serial bus (USB).

[0028] A monitor 172 or other type of display device is also connected to bus 136 via an interface, such as a video adapter 174. In addition to monitor 172, personal computers typically include other peripheral output devices (not shown), such as speakers and printers, which may be connected through output peripheral interface 175.

[0029] Computer 130 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 182. Remote computer 182 may include many or all of the elements and features described herein relative to computer 130.

[0030] Logical connections shown in Fig. 1 are a local area network (LAN) 177 and a general wide area network (WAN) 179. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets, and the Internet.

[0031] When used in a LAN networking environment, computer 130 is connected to LAN 177 via network interface or adapter 186. When used in a WAN networking environment, the computer typically includes a modem 178 or other means for establishing communications over WAN 179. Modem 178, which may be internal or external, may be connected to system bus 136 via the user input interface 170 or other appropriate mechanism.

[0032] Depicted in Fig. 1, is a specific implementation of a WAN via the Internet. Here, computer 130 employs modem 178 to establish communications with at least one remote computer 182 via the Internet 180.

[0033] In a networked environment, program modules depicted relative to computer 130, or portions thereof, may be stored in a remote memory storage device. Thus, e.g., as depicted in Fig. 1, remote application programs 189 may reside on a memory device of remote computer 182. It will be appreciated that the network connections shown and described are exemplary and other means of establishing a communications link between the computers may be used.

[0034] This description will now focus on certain aspects of the present invention for controlling the scope of delegation of authentication credentials in a client-server network environment. While the following description focuses on exemplary Kerberos-based systems and improvements there to, the various methods and systems of the present invention are also clearly applicable to other authentication systems and techniques. For example, certificate-based authentication systems and techniques may adapt certain aspects of the present invention.

[0035] As mentioned above, having possession of a client's ticket granting ticket (TGT) and associated authenticator allows the holder to request tickets on behalf of the client from the trusted third-party, e.g., a key distribution center (KDC). Such unconstrained delegation is currently supported in certain implementations of Kerberos that have forwarded ticket delegation schemes.

[0036] With this in mind, methods and systems are provided to constrain or otherwise better control the delegation process. The methods and systems can be used with different authentication protocols. The delegation process is controlled in certain exemplary implementations through a service-for-user-to-proxy (S4U2proxy) technique. The S4U2proxy technique is preferably implemented as a protocol that allows a server or service, such as, e.g., a front-end server/service, to request service tickets on behalf of a client for use with other servers/services. As described in greater detail below, the S4U2proxy protocol advantageously provides for constrained delegation in a controllable manner that does not require the client to forward a TGT to the front-end server.

[0037] Another technique provided herein is a service-for-user-to-self (S4U2self) technique. The S4U2self technique or protocol allows a server to request a service ticket to itself, but with the client's identity being provided in the resulting service ticket. This allows, for example, a client, which has been authenticated by other authentication protocols, to essentially have a service ticket that can then be used with the S4U2proxy protocol to provide constrained delegation. There are two exemplary forms to the S4U2self technique, namely a "no evidence" form and an "evidence" form. In the no evidence form, the server is trusted to authenticate the client, for example, using another security/authentication mechanism that is private to the server, for example. In the evidence form, the KDC (or a trusted-third-party) makes the authentication based on information (evidence) provided about the client obtained when the client authenticated to the server.

[0038] With the methods and systems provided herein, a client may access servers/services within a Kerberos environment regardless as to whether the client has been authenticated by Kerberos or some other authentication protocol. Consequently, back-end and/or other servers/services can be operated in an essentially Kerberos only environment.

[0039] Reference is now made to the block diagram in Fig. 2, which depicts an S4U2proxy protocol/process within a client-server environment 200, in accordance with certain exemplary implementations of the present invention.

[0040] As shown, a client 202 is operatively coupled to a trusted third-party 204 having operatively configured therein an authentication service 206, e.g., a KDC, a certificate granting authority, a domain controller, and the like. Authentication service 206 is configured to access information maintained in a database 208. Client 202 and trusted third-party 204 are further operatively coupled to a server, namely server A 210. Note, as used herein, the terms server and service are used intermixable to represent the same or similar functionality.

[0041] In this example, server A 210 is a front-end server to a plurality of other servers. Thus, as depicted, server A 210 is operatively coupled to server B 212 and server C 214. As illustrated, server B 212 may be a replicated service. Also, server C 214 is further operatively coupled to a server D 216.

[0042] In response to a user logging on at client 202, an authentication request (AS_REQ) message 220 is sent to authentication service 206, which responds with an authentication reply (AS_REP) message 222. Within AS_REP message 222, is a TGT associated with the user/client. The same or similar procedure (not illustrated) is followed to authenticate server A 210.

[0043] When client 202 wants to access server A 210, the client sends a ticket granting service request (TGS_REQ) message 224 to authentication service 206, which returns a ticket granting service reply (TGS_REP) message 226. TGS_REP message 226 includes a service ticket associated with client 202 and server A 210. Subsequently, to initiate a communication session, client 202 forwards the service ticket to server A 210, in an application protocol request (AP_REQ) message 228. Such processes/procedures are well known, and as such are not disclosed herein in greater detail.

[0044] In the past, to support delegation, the client would need to provide server A 210 with the client's TGT to allow server A 210 to request additional service tickets on behalf of client 202. This is no longer necessary. Instead, when server A 210 needs to access another server on behalf of client 202, for example, server C 214, then server A 210 and authentication service 206 operate according to the S4U2proxy protocol.

[0045] Thus, by way of example, in accordance with certain exemplary S4U2proxy protocol implementations; server A 210 sends a TGS_REQ message 230 to authentication service 206. TGS_REQ message 230 includes the TGT for server A 210 and the service ticket received from client 202, and identifies the desired or targeted server/service to which client 202 is seeking access, e.g., server C 214. In Kerberos, for example, there is a defined extensible data field, which is typically referred to as the "additional tickets" field. This additional tickets field can be used in the S4U2proxy protocol to carry the service ticket received from client 202, and a KDC options field can include a flag or other indicator that instructs the receiving KDC to look in the additional tickets field for a ticket to be used to supply a client identity. Those skilled in the art will recognize that these or other fields and/or data structures can be used to carry the necessary information to authentication service 206.

[0046] In processing TGS_REQ 230, authentication service 206 determines if client 202 has authorized delegation, for example, based on the value of a "forwardable flag" established by client 202. Thus, delegation per client is enforced by the presence of the forwardable flag in the client's service ticket. If client 202 does not want to participate in delegation, then the ticket is not flagged as forwardable. Authentication service 206 will honor this flag as a client initiated restriction.

[0047] In other implementations, authentication service 206 may access additional information in database 208 that defines selected services that server A 210 is allowed to delegate to (or not delegate to) with respect to client 202.

[0048] If authentication service 206 determines that server A 210 is allowed to delegate to the targeted server/service, then a TGS_REP message 232 is sent to server A 210. TGS_REP message 232 includes a service ticket for the targeted server/service. This service ticket appears as if client 202 requested it directly from authentication service 206, for example, using the client's TGT. However, this was not done. Instead, authentication service 206 accessed the similar/necessary client information in database 208 after being satisfied that the authenticated client is essentially involved in the request based on the service ticket that authenticated server A 210 re-

ceived from client 202 and included in TGS_REQ message 230. However, since the client information is carried in the client's ticket, the server only needs to copy the data from the ticket. Thus, database 208 can be used, but copying the data in the ticket tends to be more efficient.

[0049] In certain implementations, for example, TGS REP message 232 identifies the targeted server/service and client 202, and further includes implementation-specific identity/user/client account data, e.g., in the form of a privilege attribute certificate (PAC), a security identifier, a Unix ID, Passport ID, a certificate, etc.. A PAC, for example, may be generated by authentication service 206, or simply copied from the client's service ticket that was included in TGS_REQ message 230.

[0050] PAC or other user/client account data may also be configured to include information relating to the scope of delegation. Thus, for example, attention is drawn to Fig. 4, which is an illustrative diagram depicting selected portions of a Kerberos message 400 having a header 402 and a PAC 404. Here, PAC 404 includes delegation information 406. As illustrated, delegation information 406 includes compound identity information 408 and access restriction information 410.

[0051] Compound identity information 408 may, for example, include recorded information about the delegation process, such as, e.g., an indication regarding the fact that server A 210 requested the service ticket on behalf of user/client 202. Here, a plurality of such recorded information may be provided that can be used to string together or otherwise identify the history over multiple delegation processes. Such information may be useful for auditing purposes and/or access control purposes.

[0052] Access restriction information 410 may be used, for example, in conjunction with an access control mechanism to selectively allow access to certain servers/services provided that client 202 has either directly or indirectly through server A 210 sought to access the ser-er/service, but not if the server/service is being indirectly sought through server B 212. This feature adds additional control over the delegation of authentication credentials.

[0053] In the above examples client 202 was authenticated by authentication service 206. However, it is recognized that other clients may not be so authenticated. An example of such a situation is depicted in Fig. 3A. Here, a client 302 has been authenticated using a different authentication protocol mechanism 303. For example, authentication protocol mechanism 303 may include Passport, secure sockets layer (SSL), NTLM, Digest, or other like authenticating protocols/procedures. Here, in this example, it is assumed that client 302 chooses to access a targeted service, which just so happens to be provided by server C 214. This choice can be satisfied using the above-described S4U2proxy protocol, but only after server A 210 has completed/followed an S4U2self protocol/procedure.

[0054] One basic premise with the S4U2self protocol is that the server, e.g., server A 210, is able to request a service ticket to itself for any user/client that is accessing the server and which the server has itself authenticated. The exemplary S4U2self protocol described herein is configured to support clients that have authenticating "evidence" and clients that do not have such authenticating evidence.

[0055] In the absence of authentication evidence that can be evaluated by authentication service 206, server A 210 will need to come to "trust" client 302. Thus, for example, if client 302 has an authentication certificate or like mechanism 304 that server A 210 is able to validate, then the client 302 may be determined to be "trusted". Here, client 302 is essentially being authenticated by server A 210. Next, server A 210 sends a TGS_REQ message 306 to authentication service 206 requesting a service ticket to itself for client 302. In response, authentication service 206 generates a TGS_REP message 308 that includes the requested service ticket. The received service ticket is then used in a subsequent S4U2proxy protocol/procedure to request a service ticket to server C 214 for client 302. In certain Kerberos implementations, for example, this requires that a forwardable flag in the TGS_REP message 308 be set to allow forwarding of the service ticket. The trusted third-party may also build a PAC for client 302, which can then be included in the resulting service ticket

[0056] If evidence of the authentication does exist for a client 302', then server A 210 can include such evidence in a TGS_REQ message 312 as additional pre-authentication data. This is illustratively depicted in environment 300' in Fig. 3B. Here, evidence information 310 is provided by client 302' to server A 210. Evidence information 310 may include, for example, a challenge/response dialog, or other, information generated by another "trusted" entity. Upon receipt of evidence information 310 and subsequent validation, authentication service 206 will grant the requested service ticket to server A 210 itself. It is noted, that in certain implementations, with the use of evidence it may be possible for the server to obtain a restricted TGT for the client.

[0057] In certain Kerberos implementations, the forwardable flag in the TGS_REP message 314 will be set to allow forwarding of the service ticket. If a PAC was provided in TGS_REQ message 312, then it can be used in the service ticket, otherwise, a PAC may be generated by authentication service 206 (here, a KDC) basted an evidence information 310. For example, in S4U2self, the identity of the client is included in the pte-anthentication data. This identity can be used in the construction of the PAC for that client and added to the issued service ticket to the server (for the client).

[0058] Although some preferred implementations of the various methods and systems of the present invention have been illustrated in the accompanying Drawings and described in the foregoing Detailed Description, it will be understood that the invention is not limited to the exemplary embodiments disclosed, but is capable of numerous rearrangements, modifications and substitutions

without departing from the scope of the invention.

[0059] The following is a list of further preferred embodiments of the invention:

Embodiment 1. A method comprising:

identifying a target service to which access is sought on behalf of a client;
causing a server operatively coupled to the client to request access to the target service on behalf of the client, from a trusted third-party, wherein the server provides the trusted third-party with a credential authenticating the server, information about the target service, and a service credential previously provided by the client to the server.

Embodiment 2. The method as recited in embodiment 1, wherein the trusted third-party includes at least one service selected from a group of services comprising a key distribution center (KDC) service, a certificate granting authority service, and a domain controller service.

Embodiment 3. The method as recited in embodiment 2, wherein the trusted third-party provides the server with a new service credential granted in the name of the client rather than the server.

Embodiment 4. The method as recited in embodiment 3, wherein the new service credential is configured for use by the server and the target service to which access is sought.

Embodiment 5. The method as recited in embodiment 3, wherein the credential authenticating the server is a ticket that includes a ticket granting ticket associated with the server.

Embodiment 6. The method as recited in embodiment 1, further comprising: causing the trusted third-party to verify that the client has authorized delegation.

Embodiment 7. The method as recited in embodiment 6, wherein: the trusted third-party includes a key distribution center (KDC); and
causing the trusted third-party to verify that the client has authorized delegation includes verifying the status of a restriction placed on the ticket originating from the client.

Embodiment 8. The method as recited in embodiment 1, further comprising:

causing the trusted-third-party to selectively determine if the client is allowed to participate in delegation either based on information selected from a group comprising an identity of the client, a group affiliation associated with the client.

Embodiment 9. The method as recited in embodiment 1, wherein the server is a front-end server with respect to a back-end server that is coupled to the front-end server, and wherein the back-end server is configured to provide the target service to which access is sought.

Embodiment 10. The method as recited in embodiment 1, wherein:

the trusted third-party includes a key distribution center (KDC);
the KDC provides a ticket-granting-ticket associated with the client to the client; and
the client does not provide the ticket granting ticket to the server.

Embodiment 11. The method as recited in embodiment 1, wherein:

the trusted third-party includes a key distribution center (KDC); and
the server requests the new credential in a ticket granting service request message that includes a service ticket provided by the client to the server.

Embodiment 12. A method comprising:

identifying a target service to which access is sought on behalf of a client; and
causing a server operatively coupled to the client to request access to the target service on behalf of the client, from a trusted third party, wherein the server provides the trusted third party with a service credential authenticating the server, information about the target service, and a service credential previously provided by the client for the service, and wherein the client ticket includes implementation-specific identity information.

Embodiment 13. The method as recited in embodiment 12, wherein the implementation-specific identity information includes information selected from a group comprising privilege attribute certificate (PAC) information, security identifier information, Unix identifier information, Passport identifier information, certificate information.

Embodiment 14. The method as recited in embodiment 13, wherein the PAC information includes compound identity information.

Embodiment 15. The method as recited in embodi-

ment 13, wherein the PAC information includes access control restrictions for use as delegation constraints.

Embodiment 16. A computer-readable medium having computer-executable instructions for performing tasks comprising:

in a server, determining a target service to which access is sought on behalf of a client coupled to the server;
requesting a new service credential from a trusted third-party by providing the trusted third-party with a credential authenticating the server, information about the target service, and a service credential associated with the client and the requesting server.

Embodiment 17. The computer-readable medium as recited in embodiment 16, wherein the trusted third-party includes at least one service selected from a group of services comprising a key distribution center (KDC) service, a certificate granting authority service, and a domain controller service.

Embodiment 18. The computer-readable medium as recited in embodiment 17, wherein the new service credential is granted in the name of the client rather than the server.

Embodiment 19. The computer-readable medium as recited in embodiment 18, wherein the service credential is configured for use by the server and the target service.

Embodiment 20. The computer-readable medium as recited in embodiment 18, wherein the credential authenticating the server includes a ticket granting ticket associated with the server.

Embodiment 21. The computer-readable medium as recited in embodiment 16, further comprising:

causing the trusted third-party to verify that the client has authorized delegation.

Embodiment 22. The computer-readable medium as recited in embodiment 21, wherein:

the trusted third-party includes a key distribution center (KDC); and
causing the trusted third-party to verify that the client has authorized delegation includes verifying the status of a forwardable flag value as set by the client.

Embodiment 23. The computer-readable medium as recited in embodiment 16, wherein the server is a front-end server with respect to a back-end server coupled to the front-end server, and wherein the back-end server is configured to provide the target service.

Embodiment 24. The computer-readable medium as recited in embodiment 16, wherein:

the trusted third-party includes a key distribution center (KDC);
the KDC provides a ticket-granting-ticket associated with the client to the client; and
the client does not provide the ticket granting ticket to the server.

Embodiment 25. The computer-readable medium as recited in embodiment 16, wherein:

the trusted third-party includes a key distribution center (KDC); and
the requesting server requests the new service credential in a ticket granting service request message that includes a service ticket provided by the client to the server.

Embodiment 26. A system comprising:

a credential granting mechanism configured to receive a request for a new service credential from a server and in response generate the new service credential if delegation is allowable, and wherein the request includes:

a credential authenticating the requesting server, identifying information about a target service to which access is sought on behalf of a client coupled to the server, and a service credential that was previously granted to the client for use with the server.

Embodiment 27. The system as recited in embodiment 26, wherein the credential granting mechanism is provided by a trusted third party and includes at least one service selected from a group of services comprising a key distribution center (KDC) service, a certificate granting authority service, and a domain controller service.

Embodiment 28. The system as recited in embodiment 27, wherein the new service credential is granted in the name of the client rather than the server.

Embodiment 29. The system as recited in embodiment 28, wherein the service credential is configured for use by the server and the target service.

Embodiment 30. The system as recited in embodiment 28, wherein the credential authenticating the

server includes a ticket granting ticket associated with the server, and which was previously granted by the credential granting mechanism.

Embodiment 31. A system comprising:

a server configured to generate a request for a new service credential from a trusted third-party, the new service credential being associated with a client and a target service, the request comprising:

a credential authenticating the server, information about the target service, and a service credential associated with the client and the server.

Embodiment 32. The system as recited in embodiment 31, wherein the trusted third-party includes at least one service selected from a group of services comprising a key distribution center (KDC) service, a certificate granting authority service, and a. domain controller service.

Embodiment 33. The system as recited in embodiment 31, wherein the credential authenticating the server includes a ticket granting ticket associated with the server.

Embodiment 34. The system as recited in embodiment 31, wherein the server is a front-end server with respect to the service.

Embodiment 35. The system as recited in embodiment 31, wherein the server requests the new service credential in a ticket granting service request message that includes the service ticket associated with the client and the server.

Embodiment 36. A computer-readable medium having stored thereon a data structure, comprising:

a credential authenticating a first server,
information identifying a second server, and
a service credential associated with a client and the first server.

Embodiment 37. The computer-readable medium as recited in embodiment 36, wherein the credential authenticating the first server includes a ticket-granting-ticket (TGT) and the service credential includes a service ticket.

Embodiment 38. A method comprising:

separately authenticating a server and a client;
providing the server with a server ticket granting ticket;
providing the client with a client ticket granting ticket and a service ticket for use with the server;
providing the server with a new service ticket for use by the server for use with a new service without requiring the server to have access to the client ticket granting ticket.

Embodiment 39. The method as recited in embodiment 38, further comprising:

causing the server to request the new service ticket on behalf of the client by forwarding the server ticket granting ticket, information identifying the new service, and the service ticket to a trusted third party.

Claims

1. A method for constraining a scope of delegation by a client to a server, comprising:

identifying a target service (Server B-D) to which access is sought on behalf of a client (202) that has been authenticated using a first authentication method (303);
causing a server (210) that is operatively coupled to the target service and the client to request a service credential (303) to itself from a second authentication method based trusted third-party (204) by identifying the client and the first authentication method; and
causing the server to request from the second authentication method trusted third-party, a new service credential (308) to itself for the client, for use by the server and the target service, from the second authentication method based trusted third-party,

wherein the server provides the trusted third-party with a credential (306) authenticating the server to access the target service within a scope constrained by the client, information about the target service, and the service credential to itself.

2. The method as recited in claim 1, wherein the second authentication method based trusted third-party (204) includes at least one service (206) selected from a group of services comprising a key distribution center (KDC) service, a certificate granting authority service, and a domain controller service.

3. The method as recited in claim 2, wherein the new service credential (308) is granted in an identity of the client (202) rather than an identity of the server (210).

4. The method as recited in claim 3, wherein the new

service credential (308) is configured for use by the server (210) and the target service (Server B-D) to which access is sought.

5. The method as recited in claim 3, wherein the credential (306) authenticating the server (210) includes a ticket granting ticket associated with the server.

6. The method as recited in claim 1, further comprising:

upon receiving a request (306) for the new service credential (308) from the server (210), causing the second authentication method based trusted third-party (204) to verify that the client (202) has authorized delegation.

7. The method as recited in claim 1, wherein the server (210) is a front-end server with respect to a back-end server that is coupled to the front-end server, and wherein the back-end server is configured to provide the target service.

8. The method as recited in claim 1, wherein the first authentication method (303) is selected from a group of authentication methods comprising Passport, SSL, NTLM, and Digest.

9. The method as recited in claim 1, wherein the second authentication method (206) includes a Kerberos authentication protocol.

10. A computer-readable medium having computer-executable instructions for performing tasks comprising:

identifying a target service (Server B-D) to which access is sought on behalf of a client (202) that has been authenticated using a first authentication method (303);
causing a server (210) that is operatively coupled to the target service and the client to request a service credential (308) to itself from a second authentication method based trusted third-party (204) by identifying the client and the first authentication protocol; and
causing the server to request from the second authentication method trusted third-party, a new service credential (308) to itself for the client, for use by the server and the target service, from the second authentication method based trusted third-party, wherein the server provides the trusted third-party with a credential (306) authenticating the server to access the target service within a scope constrained by the client, information about the target service, and the service credential to itself.

11. The computer-readable medium as recited in claim 10, wherein the second authentication method based trusted third-party (204) includes a key distribution center (KDC).

12. The computer-readable medium as recited in claim 11, wherein the new service credential (308) includes a service credential granted in an identity of the client rather than an identity of the server.

13. The computer-readable medium as recited in claim 12, wherein the new service credential is configured for use by the server (210) and the target service (Server B-D).

14. The computer-readable medium as recited in claim 12, wherein the credential (306) authenticating the server (210) includes a ticket granting ticket associated with the server.

15. The computer-readable medium as recited in claim 10, further comprising:

upon receiving a request for the new service credential (308) from the server (210), causing the second authentication method based trusted third-party (204) to verify that the client(202) has authorized delegation.

16. The computer-readable medium as recited in claim 10, wherein the server (210) is a front-end server with respect to a back-end server that is coupled to the front-end server, and wherein the back-end server is configured to provide the target service (Server B-D).

17. The computer-readable medium as recited in claim 10, wherein the first authentication method (303) is selected from a group of authentication methods comprising Passport, SSL, NTLM, and Digest.

18. The computer-readable medium as recited in claim 10, wherein the second authentication method (206) includes a Kerberos authentication protocol.

19. A server system comprising:

means configured to identify a target service (Server B-D) to which access is sought on behalf of a client (202) that has been authenticated using a first authentication method (303),
means configured to request a service credential (308) to itself from a second authentication method based trusted third-party (204) by identifying the client and the first authentication method, and
means configured to subsequently request a new service credential to itself for the client, for use by the server system and the target service,

from the second authentication method based trusted third-party,
wherein the server system further comprises means configured to provide the second authentication method trusted third-party with a credential (306) authenticating the server to access the target service within a scope constrained by the client, information about the target service, and the service credential to itself.

20. The system as recited in claim 19, further comprising means configured to grant the new service credential (308) in an identity of the client(202) rather than the server system (210).

21. The system as recited in claim 20, wherein the new service credential (308) is configured for use by the server system (210) and the target service (Server B-D).

22. The system as recited in claim 20, wherein the credential (306) authenticating the server system (210) includes a ticket granting ticket associated with the server.

23. The system as recited in claim 19, wherein the server system (210) is a front-end server with respect to a back-end server that is coupled to the front-end server, and wherein the back-end server is configured to provide the target service (Server B-D).

24. The system as recited in claim 19, wherein the first authentication method (303) is one of a group of authentication methods comprising Passport, SSL, NTLM, and Digest.

25. The system as recited in claim 19, wherein the second authentication method (206) comprises means configured to use a Kerberos authentication protocol.

Patentansprüche

1. Verfahren zum Einschränken eines Bereichs von Delegation durch einen Client an einen Server, das umfasst

Identifizieren eines Ziel-Dienstes (Server B-D), zu dem Zugang im Namen eines Client (202) angefordert wird, der unter Verwendung eines ersten Authentifizierungsverfahrens (303) authentifiziert worden ist;
Veranlassen, dass ein Server (210), der funktionell mit dem Ziel-Dienst und dem Client gekoppelt ist, ein Dienst-Credential (303) an sich selbst von einer vertrauenswürdigen dritten Seite (204) auf Basis eines zweiten Authentifizierungsverfahrens anfordert, indem er den Client und das erste Authentfizierungsverfahren identifiziert; und
Veranlassen, dass der Server von der vertrauenswürdigen dritten Seite auf Basis des zweiten Authentifizierungsverfahrens ein neues Dienst-Credential (308) an sich selbst für den Client zur Verwendung durch den Server und den Ziel-Dienst von der vertrauenswürdigen dritten Seite auf Basis des zweiten Authentifizierungsverfahrens anfordert, wobei der Server der vertrauenswürdigen dritten Seite ein Credential (306) bereitstellt, das den Server zum Zugreifen auf den Ziel-Dienst innerhalb eines Bereichs authentifiziert, der durch den Client, Informationen über den Ziel-Dienst und das Dienst-Credentiat an sich selbst eingeschränkt wird.

2. Verfahren nach Anspruch 1, wobei die vertrauenswürdige dritte Seite (204) auf Basis des zweiten Authentifizierungsverfahrens wenigstens einen Dienst (206) enthält, der aus einer Gruppe von Diensten ausgewählt wird, die einen Dienst eines Schlüssel-Verteilungszentrums (KDC), einen Dienst einer Zertifikatsverteilungsbehörde und einen Dienst eines Domain-Controllers umfasst.

3. Verfahren nach Anspruch 2, wobei das neue Dienst-Credential (308) in einer Identität des Client (202) anstelle einer Identität des Servers (210) erteilt wird.

4. Verfahren nach Anspruch 3, wobei das neue Dienst-Credential (308) zur Verwendung durch den Server (210) und den Ziel-Dienst (Server B-D), auf den Zugriff angefordert wird, konfiguriert ist.

5. Verfahren nach Anspruch 3, wobei das Credential (306), das den Server (210) authentifiziert, ein Ticket zur Ticketausstellung (ticket granting ticket) enthält, das mit dem Server zusammenhängt.

6. Verfahren nach Anspruch 1, das des Weiteren umfasst:

beim Empfangen einer Anforderung (306) des neuen Dienst-Credentials (308) von dem Server (210) Veranlassen, dass die vertrauenswürdige dritte Seite (204) auf Basis des zweiten Authentifizierungsverfahrens verifiziert, dass der Client (202) über autorisierte Delegierung verfügt.

7. Verfahren nach Anspruch 1, wobei der Server (210) ein Front-End-Server in Bezug auf einen Back-End-Server ist, der mit dem Front-End-Server gekoppelt ist, und wobei der Back-End-Server zum Bereitstellen des Ziel-Dienstes konfiguriert ist.

8. Verfahren nach Anspruch 1, wobei das erste Authen-

tifizierungsverfahren (303) aus einer Gruppe von Authentifizierungsverfahren ausgewählt wird, die Passport, SSL, NTLM und Digest umfasst.

9. Verfahren nach Anspruch 1, wobei das zweite Authentifizierungsverfahren (206) ein Kerberos-Authentifizierungsprotokoll enthält.

10. Computerlesbares Medium, das durch Computer ausführbare Befehle zum Durchführen von Aufgaben aufweist, die umfassen:

Identifizieren eines Ziel-Dienstes (Server B-D), zu dem Zugang im Namen eines Client (202) angefordert wird, der unter Verwendung eines ersten Authentifizierungsverfahrens (303) authentifiziert worden ist;
Veranlassen, dass ein Server (210), der funktionell mit dem Ziel-Dienst und dem Client gekoppelt ist, ein Dienst-Credential (308) an sich selbst von einer vertrauenswürdigen dritten Seite (204) auf Basis eines zweiten Authentifizierungsverfahrens anfordert, indem er den Client und das erste Authentifizierungsprotokoll identifiziert; und
Veranlassen, dass der Server von der vertrauenswürdigen dritten Seite auf Basis des zweiten Authentifizierungsverfahrens ein neues Dienst-Credential (308) an sich selbst für den Client zur Verwendung durch den Server und den Ziel-Dienst von der vertrauenswürdigen dritten Seite auf Basis des zweiten Authentifizierungsverfahrens anfordert, wobei der Server der vertrauenswürdigen dritten Seite ein Credential (306) bereitstellt, das den Server zum Zugreifen auf den Ziel-Dienst innerhalb eines Bereichs authentifiziert, der durch den Client, Informationen über den Ziel-Dienst und das Dienst-Credential an sich selbst eingeschränkt wird.

11. Computerlesbares Medium nach Anspruch 10, wobei die vertrauenswürdige dritte Seite (204) auf Basis des zweiten Authentifizierungsverfahrens ein Schlüssel-Verteilungszentrum (KDC) enthält.

12. Computerlesbares Medium nach Anspruch 11, wobei das neue Dienst-Credential (308) eine Dienst-Credential enthält, das in einer Identität des Client anstelle einer Identität des Servers erteilt wird.

13. Computerlesbares Medium nach Anspruch 12, wobei das neue Dienst-Credential zur Verwendung durch den Server (210) und den Ziel-Dienst (Server B-D) konfiguriert ist.

14. Computerlesbares Medium nach Anspruch 12, wobei das Credential (306), das den Server (210) authentifiziert, ein Ticket zur Ticketausstellung (ticket granting ticket) enthält, das mit dem Server zusammenhängt.

15. Computerlesbares Medium nach Anspruch 10, das des Weiteren umfasst:

beim Empfangen einer Anforderung des neuen Dienst-Credential (308) von dem Server (210) Veranlassen, dass die vertrauenswürdige dritte Seite (204) auf Basis des zweiten Authentifizierungsverfahrens verifiziert, dass der Client (202) über authorisierte Delegierung verfügt.

16. Computerlesbares Medium nach Anspruch 10, wobei der Server (210) ein Front-End-Server in Bezug auf einen Back-End-Server ist, der mit dem Front-End-Server gekoppelt ist, und wobei der Back-End-Server zum Bereitstellen des Ziel-Dienstes (Server B-D) konfiguriert ist.

17. Computerlesbares Medium nach Anspruch 10, wobei das erste Authentifizierungsverfahren (303) aus einer Gruppe von Authentifizierungsverfahren ausgewählt wird, die Passport, SSL, NTLM und Digest umfasst.

18. Computerlesbares Medium nach Anspruch 10, wobei das zweite Authentifizierungsverfahren (206) ein Kerberos-Authentfizierungsprotokoll enthält.

19. Server-System, das umfasst:

eine Einrichtung, die zum Identifizieren eines Ziel-Dienstes (Server B-D) konfiguriert
ist, zu dem Zugang im Namen eines Client (202) angefordert wird, der unter Verwendung eines ersten Authentifizierungsverfahrens (303) authentifiziert worden ist,
eine Einrichtung, die zum Anforderung eines Dienst-Credentials (308) an sich selbst von einer vertrauenswürdigen dritten Seite (204) auf Basis eines zweiten Authentifizierungsverfahrens durch Identifizieren des Client und des ersten Authentifizierungsverfahrens konfiguriert ist, und
eine Einrichtung, die zum anschließenden Anfordern eines neuen Dienst-Credentials an sich selbst für den Client zur Verwendung durch das Server-System und den Ziel-Dienst von der vertrauenswürdigen dritten Seite auf Basis des zweiten Authentifizierungsverfahrens konfiguriert ist,
wobei das Server-System des Weiteren eine Einrichtung umfasst, die so konfiguriert ist, dass sie der vertrauenswürdigen dritten Seite auf Basis des zweiten Authentifizierungsverfahrens ein Credential (306) bereitstellt, das den Server zum Zugreifen auf den Ziel-Dienst innerhalb ei-

nes Bereiches authentifiziert, der durch den Client, Informationen über den Ziel-Dienst und das Dienst-Credential an sich selbst eingeschränkt wird.

20. System nach Anspruch 19, das des Weiteren eine Einrichtung umfasst, die so konfiguriert ist, dass sie das neue Dienst-Credential (308) in einer Identität des Client (202) anstelle des Server-Systems (210) erteilt.

21. System nach Anspruch 20, wobei das neue Dienst-Credential (308) zur Verwendung durch das Server-System (210) und den Ziel-Dienst (Server B-D) konfiguriert ist.

22. System nach Anspruch 20, wobei das Credential (306), das das Server-System (210) authentifiziert, ein Ticket zur Ticketausstellung (ticket granting tikket) enthält, das mit dem Server zusammenhängt.

23. System nach Anspruch 19, wobei das Server-System (210) ein Front-End-Server in Bezug auf einen Back-End-Server ist, der mit dem Front-End-Server gekoppelt ist, und wobei der Back-End-Server so konfiguriert ist, dass er den Ziel-Dienst (Server B-D) bereitstellt.

24. System nach Anspruch 19, wobei das erste Authentfizierungsverfahren (303) eines einer Gruppe von Authentifizierungsverfahren ist, die Passport, SSL, NTLM und Digest umfasst.

25. System nach Anspruch 19, wobei das zweite Authentifizierungsverfahren (206) eine Einrichtung umfasst, die so konfiguriert ist, dass sie ein Kerberos-Authentifizierungsprotokoll verwendet.

Revendications

1. Procédé pour restreindre une étendue de délégation d'un client à un serveur, comprenant les étapes qui consistent à:

identifier un service cible (Serveur B-D) pour lequel un accès est recherché pour le compte d'un client (202) qui a été authentifié à l'aide d'une première méthode d'authentification (303);
amener un serveur (210) relié de manière opérationnelle au service cible et au client à requérir un pouvoir de délégation de service (303) à son nom d'un tiers de confiance (204) en vertu d'une seconde méthode d'authentification en identifiant le client et la première méthode d'authentification; et
amener le serveur à requérir du tiers de confiance en vertu de la seconde méthode d'authentification, un nouveau pouvoir de délégation de service (308) à son nom pour le client, destiné à être utilisé par le serveur et le service cible, de la part du tiers de confiance en vertu de la seconde méthode d'authentification, le serveur fournissant au tiers de confiance un pouvoir de délégation (306) qui authentifie l'accès du serveur au service cible dans un cadre restreint par le client, des informations concernant le service cible, et le pouvoir de délégation de service à son nom.

2. Procédé tel que défini dans la revendication 1, dans lequel le tiers de confiance (204) en vertu de la seconde méthode d'authentification comprend au moins un service (206) choisi dans un groupe de services comprenant un service d'un centre de distribution de clés (KDC), un service d'une autorité de délivrance de certificats et un service d'un organe de contrôle de domaine.

3. Procédé tel que défini dans la revendication 2, dans lequel le nouveau pouvoir de délégation de service (308) est délivré au nom du client (202) et non au nom du serveur (210).

4. Procédé tel que défini dans la revendication 3, dans lequel le nouveau pouvoir de délégation de service (308) est configuré pour être utilisé par le serveur (210) et le service cible (Serveur B-D) pour lequel un accès est recherché.

5. Procédé tel que défini dans la revendication 3, dans lequel le pouvoir de délégation (306) authentifiant le serveur (210) comprend un ticket de délivrance de ticket associé au serveur.

6. Procédé tel que défini dans la revendication 1, comprenant également les étapes qui consistent à:

à la réception d'une demande (306) requérant le nouveau pouvoir de délégation de service (308) de la part du serveur (210), amener le tiers de confiance (204) en vertu de la seconde méthode d'authentification à vérifier que le client (202) a une délégation autorisée.

7. Procédé tel que défini dans la revendication 1, dans lequel le serveur (210) est un serveur frontal par rapport à un serveur dorsal qui est relié au serveur frontal, et dans lequel le serveur dorsal est configuré pour fournir le service cible.

8. Procédé tel que défini dans la revendication 1, dans lequel la première méthode d'authentification (303) est choisie dans un groupe de méthodes d'authentification comprenant Passport, SSL, NTLM et Digest.

9. Procédé tel que défini dans la revendication 1, dans lequel la seconde méthode d'authentification (206) comprend un protocole d'authentification Kerberos.

10. Support lisible par ordinateur comportant des instructions exécutables par ordinateur pour effectuer des tâches consistant à:

identifier un service cible (Serveur B-D) pour lequel un accès est recherché pour le compte d'un client (202) qui a été authentifié à l'aide d'une première méthode d'authentification (303);
amener un serveur (210) relié de manière opérationnelle au service cible et au client à requérir un pouvoir de délégation de service (308) à son nom d'un tiers de confiance (204) en vertu d'une seconde méthode d'authentification en identifiant le client et le premier protocole d'authentification; et
amener le serveur à requérir du tiers de confiance en vertu de la seconde méthode d'authentification, un nouveau pouvoir de délégation de service (308) à son nom pour le client, destiné à être utilisé par le serveur et le service cible, de la part du tiers de confiance en vertu de la seconde méthode d'authentification, le serveur fournissant au tiers de confiance un pouvoir de délégation (306) qui authentifie l'accès du serveur au service cible dans.un cadre restreint par le client, des informations concernant le service cible, et le pouvoir de délégation de service à son nom.

11. Support lisible par ordinateur tel que défini dans la revendication 10, dans lequel le tiers de confiance (204) en vertu de la seconde méthode d'authentification comprend un centre de distribution de clés (KDC).

12. Support lisible par ordinateur tel que défini dans la revendication 11, dans lequel le nouveau pouvoir de délégation de service (308) comprend un pouvoir de délégation de service délivré au nom du client et non au nom du serveur.

13. Support lisible par ordinateur tel que défini dans la revendication 12, dans lequel le nouveau pouvoir de délégation de service est configuré pour être utilisé par le serveur (210) et le service cible (Serveur B-D).

14. Support lisible par ordinateur tel que défini dans la revendication 12, dans lequel le pouvoir de délégation (306) authentifiant le serveur (210) comprend un ticket de délivrance de ticket associé au serveur.

15. Support lisible par ordinateur tel que défini dans la revendication 10, comprenant également des instructions pour:

à la réception d'une demande requérant le nouveau pouvoir de délégation de service (308) de la part du serveur (210), amener le tiers de confiance (204) en vertu de la seconde méthode d'authentification à vérifier que le client (202) a une délégation autorisée.

16. Support lisible par ordinateur tel que défini dans la revendication 10, dans lequel le serveur (210) est un serveur frontal par rapport à un serveur dorsal qui est relié au serveur frontal, et dans lequel le serveur dorsal est configuré pour fournir le service cible (Serveur B-D).

17. Support lisible par ordinateur tel que défini dans la revendication 10, dans lequel la première méthode d'authentification (303) est choisie dans un groupe de méthodes d'authentification comprenant Passport, SSL, NTLM et Digest.

18. Support lisible par ordinateur tel que défini dans la revendication 10, dans lequel la seconde méthode d'authentification (206) comprend un protocole d'authentification Kerberos.

19. Système serveur comprenant:

un moyen configuré pour identifier un service cible (Serveur B-D) pour lequel un accès est recherché pour le compte d'un client (202) qui a été authentifié à l'aide d'une première méthode d'authentification (303),
un moyen configuré pour requérir un pouvoir de délégation de service (308) à son nom d'un tiers de confiance (204) en vertu d'une seconde méthode d'authentification en identifiant le client et la première méthode d'authentification, et
un moyen configuré pour requérir ensuite un nouveau pouvoir de délégation de service à son nom pour le client, destiné à être utilisé par le système serveur et le service cible, de la part du tiers de confiance en vertu de la seconde méthode d'authentification,
le système serveur comprenant également un moyen configuré pour fournir au tiers de confiance en vertu de la seconde méthode d'authentification un pouvoir de délégation (306) qui authentifie l'accès du serveur au service cible dans un cadre restreint par le client, des informations concernant le service cible, et le pouvoir de délégation à son nom.

20. Système tel que défini dans la revendication 19, comprenant également un moyen configuré pour délivrer le nouveau pouvoir de délégation de service (308) au nom du client (202) et non au nom du système serveur (210).

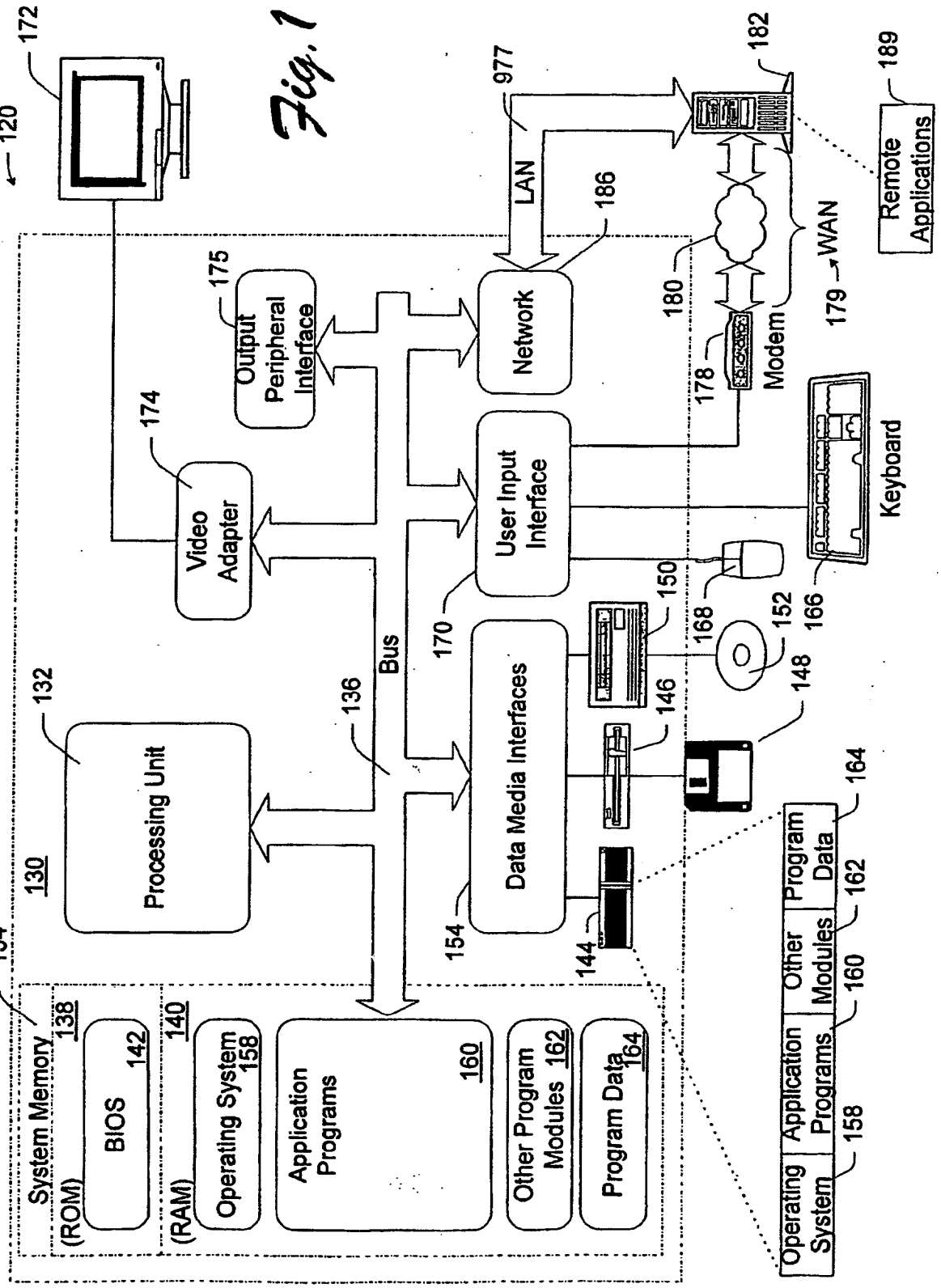
21. Système tel que défini dans la revendication 20, dans lequel le nouveau pouvoir de délégation de service (308) est configuré pour être utilisé par le système serveur (210) et le service cible (Serveur BD).

22. Système tel que défini dans la revendication 20, dans lequel le pouvoir de délégation (306) authentifiant le système serveur (210) comprend un ticket de délivrance de ticket associé au serveur.

23. Système tel que défini dans la revendication 19, dans lequel le système serveur (210) est un serveur frontal par rapport à un serveur dorsal qui est relié au serveur frontal, et dans lequel le serveur dorsal est configuré pour fournir le service cible (Serveur BD).

24. Système tel que défini dans la revendication 19, dans lequel la première méthode d'authentification (303) est l'une d'un groupe de méthodes d'authentification comprenant Passport, SSL, NTLM et Digest.

25. Système tel que défini dans la revendication 19, dans lequel la seconde méthode d'authentification (206) comprend un moyen configuré pour utiliser un protocole d'authentification Kerberos.


120
172
Fig. 1
977
182
189
LAN
186
Remote Applications
175
Output Peripheral Interface
Network
180
WAN
179
174
Modem
178
Video Adapter
User Input Interface
Keyboard
150
152
166
168
170
Bus
132
136
Processing Unit
146
148
130
Data Media Interfaces
154
144
164
134
System Memory
138
(ROM)
BIOS
142
140
(RAM)
Operating System
158
Application Programs
160
Other Program Modules
162
Program Data
164
Operating System
158
Application Programs
160
Other Modules
162
Program Data
164

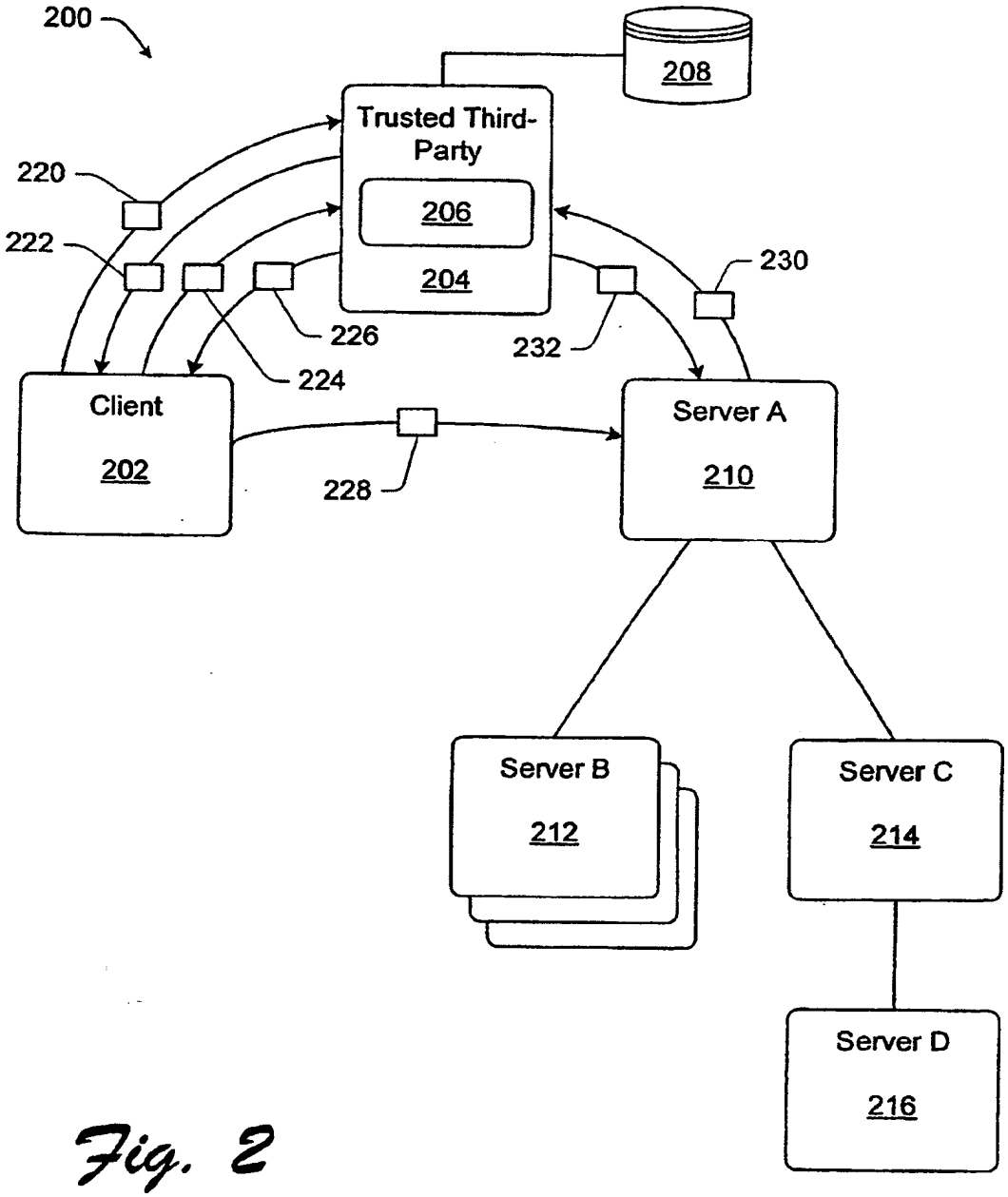

200
208
Trusted Third-Party
206
204
220
222
226
224
232
230
Client
202
228
Server A
210
Server B
212
Server C
214
Server D
216

Fig. 2

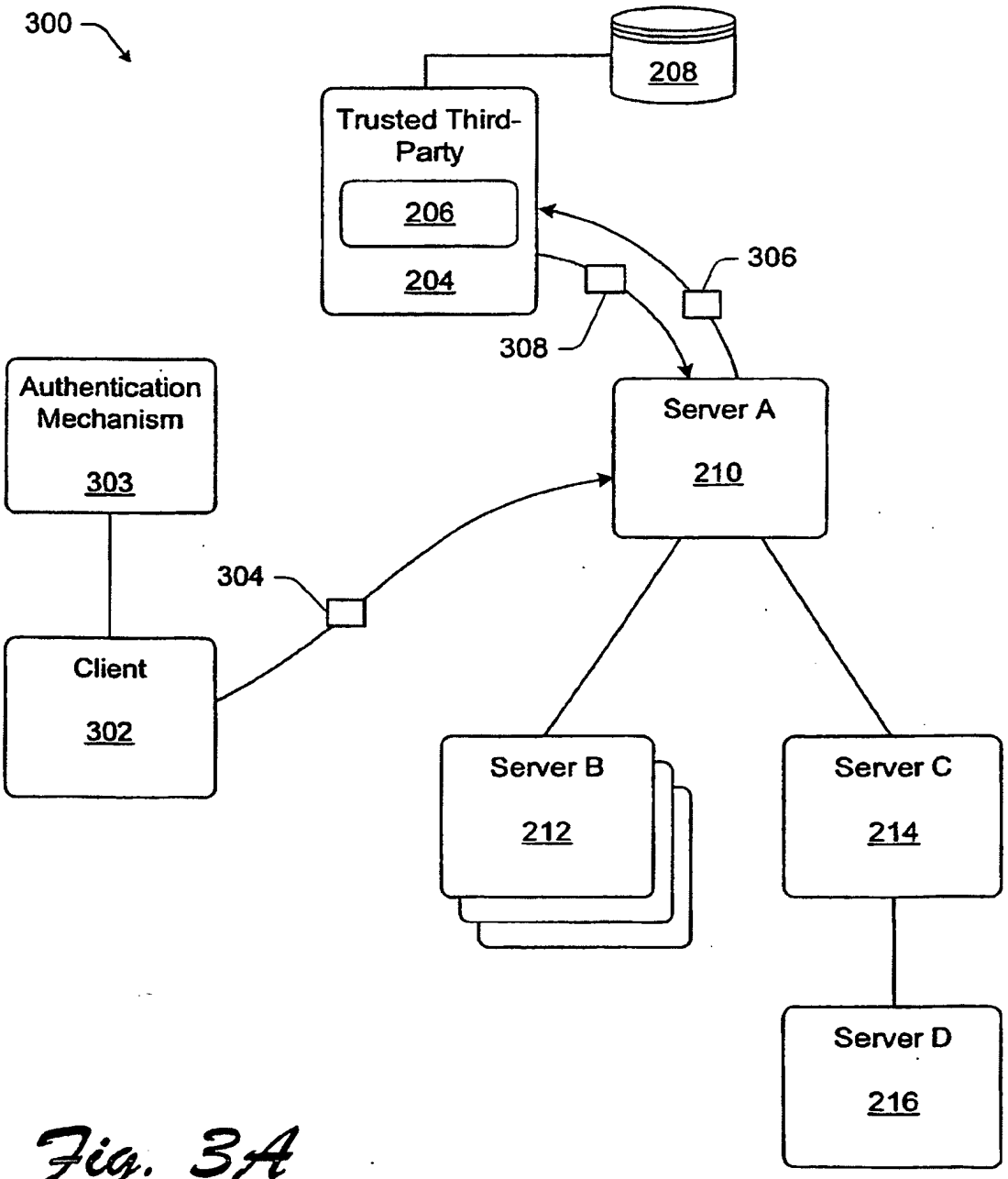

300
208
Trusted Third-Party
206
204
306
308
Authentication Mechanism
303
Server A
210
304
Client
302
Server B
212
Server C
214
Server D
216

Fig. 3A

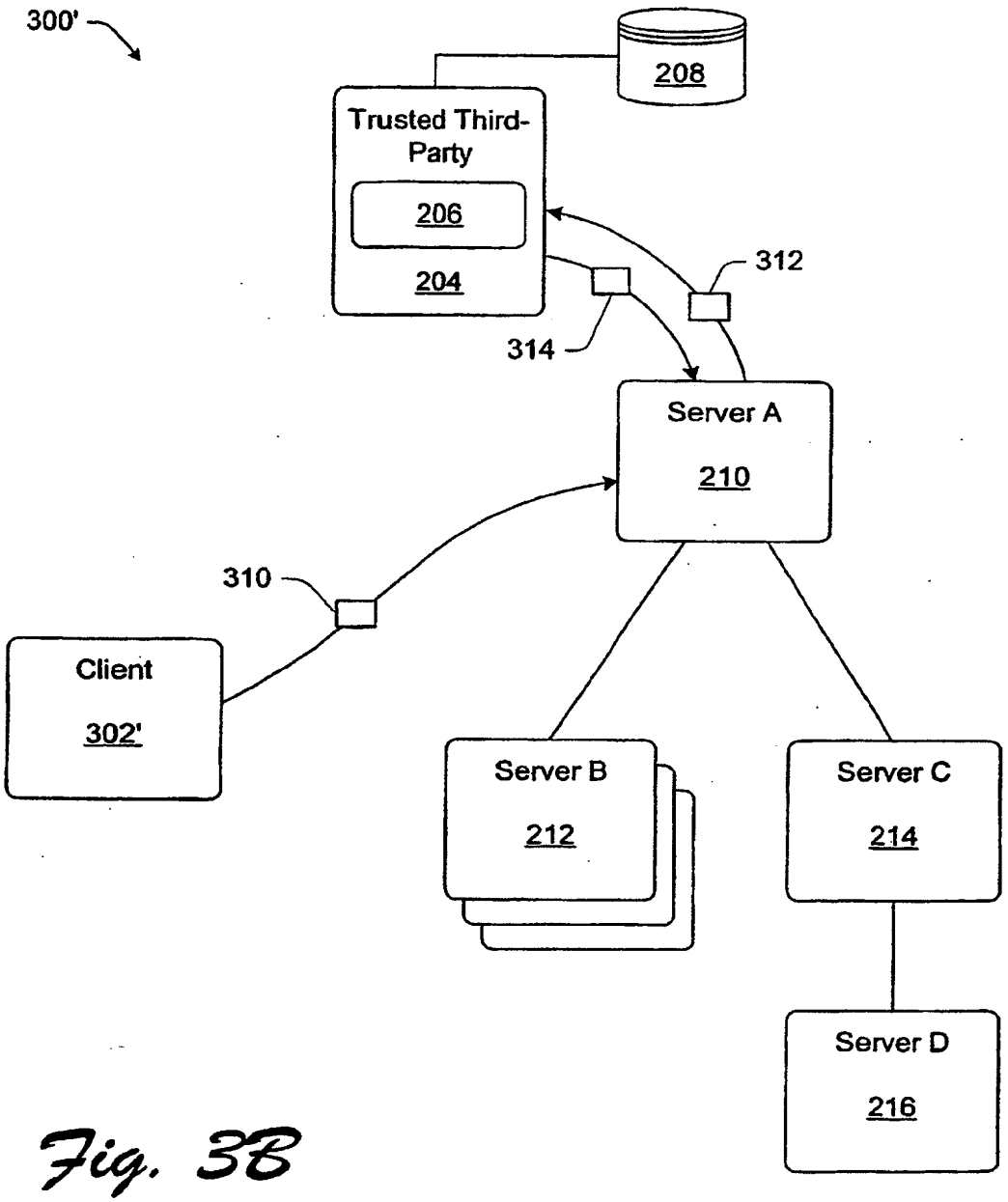

300'
208
Trusted Third-Party
206
204
312
314
Server A
210
310
Client
302'
Server B
212
Server C
214
Server D
216

Fig. 3B

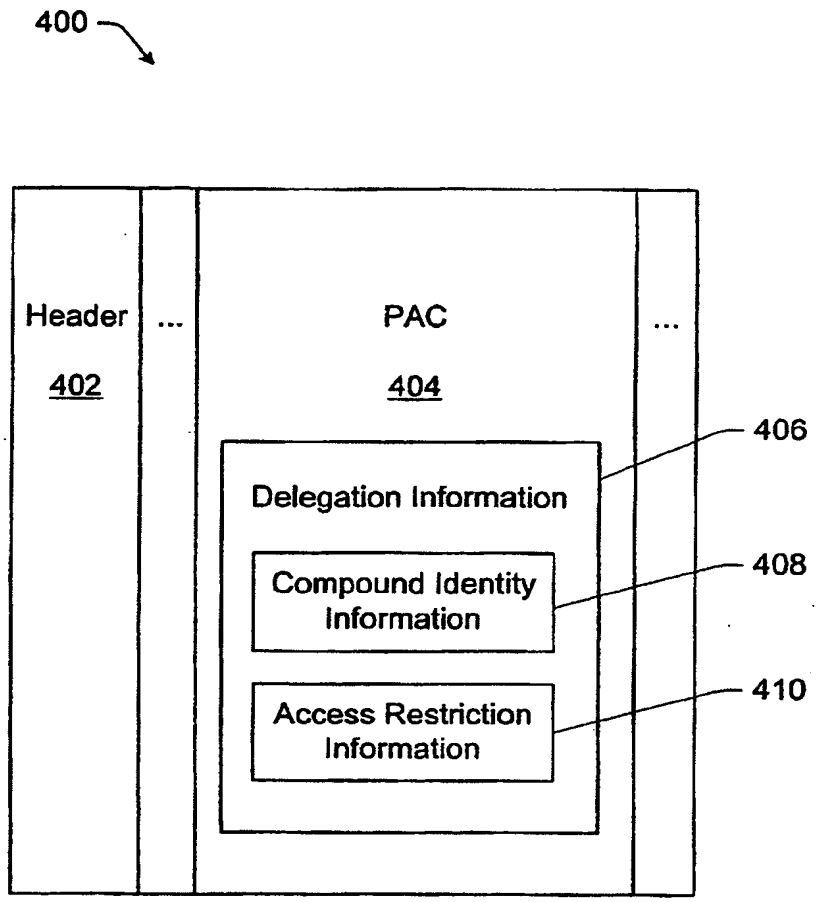

400
Header
402
...
PAC
404
...
Delegation Information
406
Compound Identity Information
408
Access Restriction Information
410

Fig. 4

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Non-patent literature cited in the description

- **MCMAHON P.V.** *SESAME V2 Public Key and Authorization Extensions to Kerberos,* 16 February 1995 **[0007]**